Public Knowledge

October 2, 2016

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: WC Docket No. 16-106

Dear Ms. Dortch:

On September 28, 2016, Harold Feld and Dallas Harris of Public Knowledge (collectively "PK") met with Wireline Bureau Chief Matthew DelNero, Lisa Hone of the Wireline Bureau, Ruth Milkman, Chief of Staff to Chairman Wheeler, and Gigi Sohn, Counselor to the Chairman, with regard to the above captioned proceeding.

Sources of Commission Authority

As the Public Knowledge has stated on numerous occasions, the Commission has multiple sources of authority for the proposed privacy rules. Accordingly, to the extent the Commission makes determinations as to the scope of its rules, it should make clear that its actions do not foreclose subsequent rulemakings or enforcement proceedings under different statutory authority. E.g., rules promulgated under 47 U.S.C. §222 do not foreclose separate enforcement proceedings under 47 U.S.C. §605.

Additionally, in the same way that the Commission made each portion of the Open Internet rules severable from all others in the event of an adverse determination by a reviewing court, the Commission should make clear that it intends its proposed privacy rules to be severable. E.g., if a reviewing court finds that the statute does not permit the FCc to adopt the FTC's "sensitive/non-sensitive" distinction, the Commission intends that the notice requirements should continue to apply.

De-Identification/Anonymization

"Congress does not hide elephants in mouse holes." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000). Had Congress intended to create a third category of information separate from the three types of data explicitly provided for in the statute ("proprietary information," "customer proprietary network information," and "aggregate data"), Congress would certainly have said so. The far better reading of 222(c)(1) is that "individually identifiable customer proprietary network information" is in contrast to aggregate information, and prohibits release of any individually identifiable information even if it is collected as part of the process of collecting aggregate information. This language is necessary – and not mere surplusage -- because the statute already prohibits the collection of CPNI as non-aggregate information (outside

of the listed exceptions) without consent. Accordingly, Section 222(c)(1) prohibits the collection of individual CPNI without consent, or the collection and release of aggregate information in a manner that exposes individually identifiable CPNI.

For example, the prohibition on the collection of individual information prevents an ISP from collecting information (without consent) from customer Jane Doe when that information is collected from no one else. The prohibition on collecting "individually identified CPNI" prevents releasing Jane Doe's information when it is collected as part of an aggregate information collection from more than one customer.

If the Commission reads this statutory language as permitting release of information collected from all customers for an individual customer (or to use that information to target a specific customer for marketing purposes), the Commission must ensure that it remains de-identified. This includes regulation of the BIAS provider to prohibit circumvention by handing di-identified information to 3rd parties for the 3rd parties to re-identify, and to conclude that failure to act when a BIAS provider discovers a third party violating the terms of its agreements violates the statute.

Use of Sensitive/Non-Sensitive Distinction

Congress made no distinction in the statute for "sensitive" and "non-sensitive" information. To the contrary, the only distinctions made by Congress are the distinctions between information provided by other telecommunications carriers to provide service under Section 222(b), and information provided by customers to receive telecommunications services. Additionally, information considered not sensitive today can easily become considered sensitive tomorrow as the broader internet of things (IoT) more deeply penetrates into our every day lives.

A BIAS provider can easily determine the type of device that attaches to the network. Devices are generally designed to identify themselves so that those managing their networks, including consumers managing their home networks, can properly configure their home networks and security systems (by recognizing foreign attachments, or to identify "rogue" devices within a network). Identification of the *type* of device, as well as the application and browser history, can reveal extremely sensitive information.

For example, numerous "smart" sex toys now operate via Bluetooth connection to a smartphone so that long distance couples can participate with each other over the internet.[1] These toys also store and transmit data on use frequency, settings and other extremely personal information.[2] It is not difficult to foresee that, as the IoT expands, devices linked to medical functions or other highly sensitive functions will proliferate and become common. The knowledge of the device itself, not simply an application run on the device or a website visited by the device,

[1] Jennifer Craig, Surviving LDR: Women's Guide on Surviving Long Distance Relationship, "5 Best Long Distance Relationship Sex Toys." Available at http://surviveldr.com/intimacy/long-distance-relationship-sex-toys/ (last visited September 29, 2016).

[2] Hudson Hongo, "Smart Sex Toy Maker Sued For Sneakily Collecting 'Intimate' Data." Forbes (September 12, 2016). Available at: http://gizmodo.com/smart-sex-toy-maker-sued-for-sneakily-collecting-intima-1786559792 (last visited September 29, 2016).

would be considered highly private information by a user. Failure to protect the privacy of devices is likely to discourage their use – even if these devices are life saving devices.[3]

Similarly, as cars increasingly connect to mobile networks, consumers consider the source of the signal, their car, as confidential. Consumers do not generally anticipate that a BIAS provider may access information about one's automobile via a Bluetooth connection with a mobile device, but collection of car information via a hands free Bluetooth connection is trivially easy.[4] Information about the make and model of the car, unique identifiers that allow advertisers or others to learn the driving patterns and habits of the mobile subscriber, are confidential information that a customer wishes protected regardless of whether the information is traditional "geolocation" information or collected in other ways.

Requirement For Reasonable Security Precautions

The Commission does not propose to change its general requirement that BIAS providers take reasonable precautions from what the Commission adopted in the 2007 Pretexting Order.[5] Where the Commission simply reaffirms its traditional interpretation of the statute, that does not open the Commission's previous interpretation to new and untimely review.

Further, the requirement that BIAS providers take "reasonable" precautions as judged by the industry standard does nothing more than to reiterate the usual standard for liability that courts routinely employ in tort law, contract law and consumer protection law. Indeed, under the FTC itself factors in the question of the industry standard for reasonable precautions when considering whether a business has violated Section 5.[6] Similarly, Section 201(b) of the Communications Act renders any "unjust or unreasonable" practice in association with providing a telecommunications service unlawful – a standard that consumers may enforce in the courts as well as before the Commission.[7]

The Commission should therefore reject any argument advanced by carriers that the Commission lacks authority to require reasonable precautions to protect the privacy of information from exposure or cyber threats. Such language is neither too vague, nor beyond the Commission's authority. To the contrary, as the Commission has previously concluded (and the

---

[3] *See* Rafi Goldberg, Policy Analyst, NTIA, "Lack of Trust In Internet Privacy and Security May Deter Economic and Other /Online Activites," (May 13, 2016). Available at: http://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (last visited September 29, 2016).

[4] *See* Lisa Weintraube Schifferle, FTC Division of Consumer Education, "What Is Your Phone Telling Your Rental Car," FTC Blog (August 30, 2016). Available at: https://www.consumer.ftc.gov/blog/what-your-phone-telling-your-rental-car (last visited September 29, 2016) (discussing information transfers between the mobile phones and rental cars).

[5] Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info., 22 F.C.C. Rcd. 6927 (2007) ¶¶37-66.

[6] *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3rd Cir. 2015). *See also* 15 U.S.C. §45(n) (requiring FTC to look to prevailing industry practices).

[7] *See* 47 U.S.C. §207 (providing any party aggrieved by common carrier conduct with a right to file before the Commission or in the federal courts). Indeed, given that carriers have made prolific use of mandatory arbitration clauses, it is only through Commission action that a subscriber can find relief from unreasonable disregard for common sense precautions to secure the privacy of user data.

D.C. Circuit has affirmed), where Congress directs the Commission to accomplish a particular goal, it grants the Commission the necessary authority to achieve the goal.[8]

Need To Address Mandatory Arbitration Clauses

In the wake of the Ninth Circuit's recent decision in *AT&T Mobility v. FTC*, the Commission has lost a valuable partner in protecting the privacy of broadband subscribers. Furthermore, the Commission relies exclusively on private rights of action and class actions to enforce MVPD privacy under 47 U.S.C. §§ 338(i) & 551. Without the ability to sue for relief in court, consumers have no replacement for the loss of the FTC as a partner with the FCC. Furthermore, the proliferation of mandatory arbitration clauses effectively forecloses consumers from enforcing their rights under 47 U.S.C. §§ 338(i) & 551.

The Commission should therefore use its authority pursuant to Section 201(b), 338(i) and 631 to prohibit enforcement of mandatory arbitration clauses. At a minimum, even if the Commission were to determine that it did not intend to prohibit such clauses based on the record, the Commission should clarify that it has such authority and will revisit its determination if evidence of the abusive effects of these clauses becomes more manifest.

In accordance with Section 1.1206(b) of the Commission's rules, this letter is being filed with your office. If you have any further questions, please contact me at (202) 861-0020.

Respectfully submitted,

/s/ Harold Feld
Harold Feld
Senior V.P.
Public Knowledge
1818 N Street, NW
Washington, DC 20036

Cc: Matthew Delnero
Lisa Hone
Ruth Milkman
Gigi Sohn

[8] *See Verizon v. FCC,* 740 F.3d 643 (D.C. Cir. 2014) (affirming FCC authority to promulgate rules to achieve the goal of 47 U.S.C. §1302).